

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Black Samsung cell phone, Model SM-S134DL(GP),
currently located at Deschutes County Sheriff's Office
Property Room, 63333 W. Hwy 20, Bend, Oregon

Case No. 3:23-mc-983

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Black Samsung cell phone, Model SM-S134DL(GP), currently located at Deschutes County Sheriff's Office Property Room, 63333 W. Hwy 20, Bend, Oregon, as described in Attachment A located in the _____ District of _____ Oregon, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 113(a)(3), (a)(6)	Assault with a Dangerous Weapon, Assault Resulting in Serious Bodily Injury
21 U.S.C. §841(a)(1)	Possession with Intent to Distribute Methamphetamine
21 U.S.C. § 843	Use of Communication facility in commission of a crime - felony

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

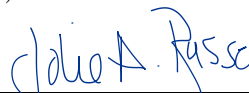
RYAN C. HALL, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone at 4:05 pm (specify reliable electronic means).

Date: November 9, 2023

City and state: Portland, Oregon


Judge's signature

HON. JOLIE A. RUSSO, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss:

AFFIDAVIT OF RYAN C. HALL

**Affidavit in Support of an Application
for a Search Warrant for a Phone**

I, Ryan C. Hall, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since May 2017. I am presently assigned to the Portland Division of the FBI, and specifically to the Salem Resident Agency. During my employment, I have investigated and have assisted others in investigating a range of federal crimes, including drug and gang-related offenses; felons in possession of a firearm; child pornography; online enticement of minors; and interstate travel for the purpose of engaging in illicit sexual activity with minors; I have conducted numerous threat assessments that have been reported to the FBI.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of a black Samsung, Model: SM-S134DL(GP), IMEI: 351966629303618 (hereinafter “Phone”), which is currently in law enforcement custody at Deschutes County Sheriff’s Office, as described in Attachment A hereto, and the extraction of electronically stored information from the Phone, as described in Attachment B hereto. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence, contraband, fruits, and instrumentalities of violations of 21 U.S.C. § 843(b) and the use of a Communication Facility to commit the offenses, 21 U.S.C. § 841(a)(1), Possession with the Intent to Distribute Controlled Substances, 18 U.S.C. § 113(a)(3), Assault with a Dangerous Weapon, and 18 U.S.C. § 113(a)(6), Assault Resulting in Serious Bodily Injury.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 18, United States Code, Section 113(a)(3), Assault with a Dangerous Weapon, makes it unlawful for an individual, within the special maritime and territorial jurisdiction of the United States, to commit an assault, by intentionally striking or wounding another with a dangerous weapon, with intent to do bodily harm.

5. Title 18, United States Code, Section 113(a)(6), Assault Resulting in Serious Bodily Injury, makes it unlawful for an individual, within the special maritime and territorial jurisdiction of the United States, to commit an assault by intentionally striking or wounding another, resulting in serious bodily injury.

6. Title 21, United States Code, Section 841(a)(1), Possession with the Intent to Distribute Controlled Substances, makes it unlawful to possess with the intent to distribute methamphetamine, a Schedule II controlled substance.

///

///

///

7. Title 21, United States Code, Section 843(b), it shall be unlawful for any person knowingly or intentionally to use any communication facility in committing or in causing or facilitating the commission of any act or acts constituting a felony under any provision of this subchapter or subchapter II.

Statement of Probable Cause

8. On June 27, 2023, at 4:25 a.m., Officers of the Warm Springs Police Department (WSPD) were dispatched to 1864 Poosh Avenue, Warm Springs, Oregon, within the boundaries of the Warm Springs Indian Reservation, following reports of a shooting. When Officers arrived, they discovered Adult Victim 1 (AV1) and Adult Victim 2 (AV2) in the residence. AV2 was on the floor in the hallway and stated that s/he had been shot in the face. Officers noticed blood on the floor and walls of the residence. AV1 told Officers that Paul Martinez shot AV2. AV1 was interviewed and stated that around 4:20 a.m, Paul Martinez and Vanessa Plazola arrived at 1864 Poosh Avenue to check on who is believed to be Plazola's son, Adult Witness (AW) and two teenage females. When they arrived, there was a verbal argument in the driveway between Martinez, Plazola, and AV1. Plazola said that she was going to get a firearm. Martinez ran into the house and started assaulting AV2, and Plazola struck AV1 in the head and arm with a piece of lumber that had been used to secure an air conditioning unit. AV1 attempted to break up the fight between Martinez and AV2 and Martinez retrieved a gun from his person and shot AV2 in the face at close range.

9. On June 27, 2023, Portland FBI SWAT personnel executed a search warrant on 2222 Elliott Heights, Warm Springs, Oregon. During the execution of the search warrant, FBI Crisis Negotiation Team (CNT) personnel contacted Plazola by telephone. An individual with a

female sounding voice answered the call, and the Agent identified himself, the reason for the call, and who he was attempting to contact. The individual believed to be Plazola terminated the call. When the Agent attempted to again contact the person believed to be Plazola, the phone call went unanswered.

Federal Grand Jury Indictment

10. On July 19, 2023, Plazola was indicted by Federal Grand Jury in the District of Oregon, case 3:23-cr-00240-02-SI, for the following offenses: Title 18 U.S.C. § 113(a)(3) “Assault with a Dangerous Weapon,” makes it unlawful for an individual, within the special maritime and territorial jurisdiction of the United States, to commit an assault, by intentionally striking or wounding another with a dangerous weapon, with intent to do bodily harm, and Title 18 U.S.C. § 113(a)(6) “Assault Resulting in Serious Bodily Injury,” makes it unlawful for an individual, within the special maritime and territorial jurisdiction of the United States, to commit an assault by intentionally striking or wounding another, resulting in serious bodily injury.

11. On October 11, 2023, Plazola was indicted by Federal Grand Jury in the District of Oregon, case 3:23-cr-00327-SI, for the following offense: Title 21, U.S.C. §§ 841(a)(I) and 841(b)(I)(A), unlawfully, knowingly, and intentionally possess with the intent to distribute 500 grams or more of a mixture and substance containing a detectable amount of methamphetamine, a Schedule II controlled substance.

Deschutes County CODE Investigation

12. During an unrelated investigation, state law enforcement officers were monitoring a Deschutes County inmate’s phone calls. The inmate, arrested on August 25, 2023, engaged in several voice and video calls with phone number (458) 292-9457. This phone number is

registered to Vanessa Plazola through Telemate, a service that collects data on the individuals who inmates have contact with. A Deschutes County Sheriff's Detective compared video images of Plazola to the video calls and positively identified the caller as Plazola. The inmate also referred to Plazola as Vanessa on several occasions.

13. On September 14, 2023, I applied for and received a geolocation warrant, 3:23-mc-791, for phone number (458) 292-9457. I began tracking the phone's location based on location data and disseminated the information to the Central Oregon Drug Enforcement (hereinafter referred to as, "CODE") team. CODE detectives began surveillance operations based on location data. On September 18, 2023, CODE detectives applied for and received a search warrant for any vehicles associated with Plazola and for Plazola's person. On that same day, at or around 11:06 am, investigators observed that the location data on Plazola's cell phone showed her traveling west through Sisters, Oregon towards Salem, Oregon. CODE surveillance units attempted to follow the location data on the cell phone in an attempt to determine the vehicle Plazola was using. Surveillance units drove to Salem and then followed the location data to Portland, but they were unable to locate Plazola or the vehicle due to the heavy traffic and the wide radius of the location data. Later that evening, CODE surveillance units returned to Deschutes County, Oregon, with Plazola's phone location data still pinging in the Portland area.

14. On September 19, 2023, at approximately 8:00 p.m., investigators observed that the location data was moving east towards Sandy, Oregon. Based on the direction of travel, CODE detectives ascertained that Plazola was like driving in the direction of Deschutes County, Oregon. CODE surveillance units were deployed throughout Jefferson County, Oregon to identify Plazola's vehicle. Based on location data and physical surveillance, CODE detectives

were able to identify the vehicle as a gray, 2011 Dodge Charger bearing Washington License Plate: BYF1388. CODE detectives surveilled the vehicle in Jefferson County, Oregon. CODE detectives lost sight of the vehicle for a period of time as they were unable to follow it due to the rural roads and time of day. Eventually, CODE detectives were able to re-acquire the vehicle in vicinity of Bear Dr in Madras, Oregon. CODE detectives observed the Dodge Charger travelling in tandem with a second vehicle as they drove south. CODE detectives advised other surveillance units in the area of the vehicles location.

15. CODE continued to follow the vehicles loosely knowing that they had to pass over the high bridge at the Deschutes County, Oregon line. Once the vehicle was seen crossing the high bridge, CODE detectives had DCSO marked units set up for a traffic stop. Marked units got behind the vehicle and initiated a traffic stop in Terrebonne, Oregon. At that time, the vehicle that was in tandem with the Charger pulled over and stopped. The Dodge Charger fled from DCSO units, leading them on a high-speed pursuit. The pursuit was eventually terminated when the vehicle entered Crook County, Oregon and pursuing units lost sight of the vehicle in the area of O' Neil Hwy and Overland Ranch Rd. Marked and unmarked units circulated the area looking for the vehicle for several minutes before a 911 call came in advising that there was a vehicle in the driveway of a house at 3791 Lexie Ln, Powell Butte, Oregon. CODE detectives, along with several patrol units, responded to that location. Once the passenger in the car was detained, DCSO detectives conducted a search of the vehicle pursuant to a Deschutes County Circuit Court search warrant. When CODE detectives searched the Charger, they found that the driver side door was open. CODE detectives located several glass pipes commonly used to smoke methamphetamine, as well as some packaging material in the glove box of the vehicle.

CODE detectives also located a suitcase in the trunk with women's clothing and accessories. DCSO units flew drones over the area and attempted to track and locate Plazola for about an hour.

16. DCSO continued to search for Plazola into the early morning hours of September 20, 2023. DCSO drone operators located a female walking along an irrigation pivot near where the Dodge Charger was abandoned. CODE detectives, as well as DCSO patrol units, drove to that location and eventually located Plazola hiding in an unlocked vehicle that was parked on the property near the pivot. Plazola was called out of the vehicle. Plazola held the Phone in her right hand and was instructed to drop it. The Phone was seized at time of arrest, put into faraday, and is in lawful custody of DCSO. Furthermore, DCSO deputies and CODE detectives located a purse in the unlocked vehicle where Plazola was located. Plazola affirmed the purse belonged to her. Inside the purse, CODE detectives located suspected methamphetamine. Plazola was transported to Deschutes County Jail where she was booked. CODE detectives later arrived at DCSO where they obtained gross weights of 421.16 grams and 453.16 grams of suspected methamphetamine. CODE detectives used a NIK test kit to obtain a presumptive positive result for methamphetamine. CODE detectives then booked the drug evidence into the DCSO property room.

Interview of Vanessa Plazola

17. On September 20, 2023, Plazola was interviewed at the Deschutes County Jail. Prior to the start of the interview, FBI SA Nick Oliver recited verbal Miranda warnings, and Plazola affirmed her understanding of her rights and consented to be interviewed.

18. The Phone is currently in storage at Deschutes County Sheriff's Office. In my training and experience, I know that the Phone has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Phone first came into the possession of the Deschutes County Sheriff's Office.

19. Based on my training and experience, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet,¹ including the use of apps.² Wireless telephones may also include a global positioning system ("GPS") technology for determining the location of the device.

¹ The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

² Apps is an abbreviation for applications. An app is a self-contained program or piece of software designed to fulfill a particular purpose. An app can run on the Internet, on a computer, on a cell phone, or on other electronic devices.

20. Based on my training, experience, and research, I know that the Phone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, etc. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, and the purpose of its use.

21. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Phone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Phone because, based on my knowledge, training, and experience, I know:

a. Phones can store information for long periods of time, including information viewed via the Internet. Files or remnants of files can be recovered with forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person “deletes” a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, the Phone may contain electronic evidence of how it has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Data on the Phone can provide evidence of a file that was once on the Phone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on the Phone that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the Phone that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and the times the Phone was in use. File systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

f. A person with appropriate familiarity with how the Phone works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the Phone was used, the purpose of its use, who used it, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data

stored on the Phone is evidence may depend on other information stored on the Phone and the application of knowledge about how a Phone functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in order to find evidence of how the Phone was used, the purpose of its use, who used it, and when, the examiner may have to establish that a particular thing is not present on the Phone.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Phone consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Phone and computer-assisted scans and searches of the entire Phone that might expose many parts of the device to human inspection in order to determine whether it constitutes evidence as described by the warrant.

23. The initial examination of the Phone will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

24. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phone or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without

authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

25. If an examination is conducted, and it is determined that the Phone does not contain any data falling within the ambit of the warrant, the government will return the Phone to its owner within a reasonable period of time following the search and will seal any image of the Phone, absent further authorization from the Court.

26. If the Phone contains evidence, fruits, contraband, or is an instrumentality of the crime, the government may retain the Phone as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phone and/or the data contained therein.

27. The government will retain a forensic image of the Phone for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

28. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

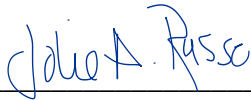
29. Based on the foregoing, I have probable cause to believe, and I do believe, that the Phone described in Attachment A contains evidence, contraband, fruits, and instrumentalities of violations of Title 21 U.S.C. § 843(b) and the use of a Communication Facility to commit the offenses, Title 21, U.S.C. Section 841(a)(1), Possession with the Intent to Distribute Controlled Substances, 18 U.S.C. §§ 113(a)(3), Assault with a Dangerous Weapon, and Title 18 U.S.C. 113(a)(6), Assault Resulting in Serious Bodily Injury, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Phone described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

30. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Pam Paaso, and AUSA Paaso advised me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By telephone
Ryan C. Hall
Special Agent, FBI

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at

4:05 pm November 9, 2023.

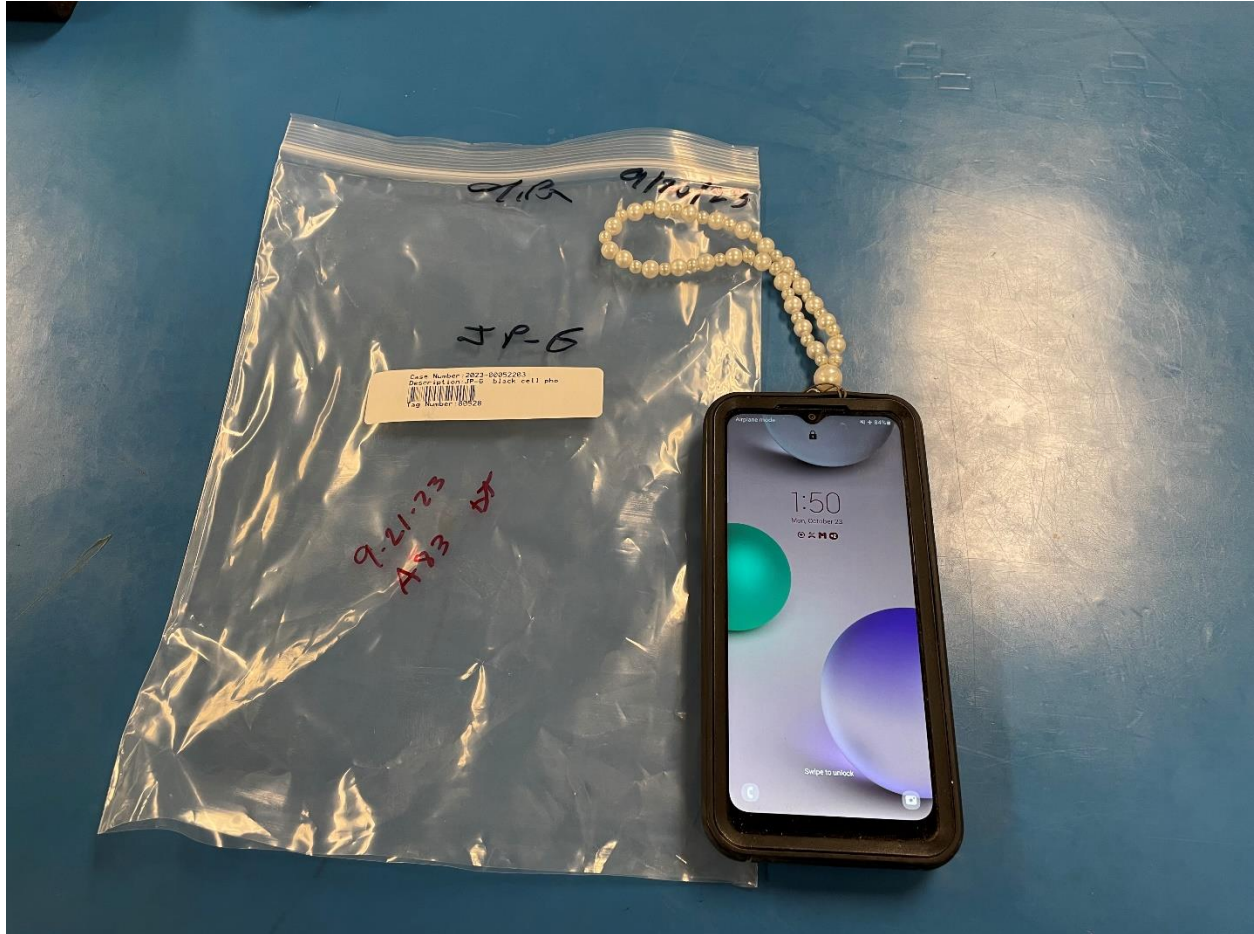


HON. JOLIE A. RUSSO
United States Magistrate Judge

ATTACHMENT A

Phone to Be Searched

The phone to be searched is a black Samsung, Model: SM-S134DL(GP),
IMEI: 351966629303618 and is currently located on the premises of Deschutes County Sheriff's
Office Property Room at 63333 W. Hwy 20 in Bend, Oregon.



Attachment A



Attachment A

ATTACHMENT B

Items to Be Seized

1. All records on the Phone(s) described in Attachment A that relate to violations of Title 21 U.S.C. Section 843(b) and the use of a Communication Facility to commit the offenses, Title 21, U.S.C. Section 841(a)(1), Possession with the Intent to Distribute Controlled Substances, 18 U.S.C. Section 113(a)(3), Assault with a Dangerous Weapon, and Title 18 U.S.C. Section 113(a)(6), Assault Resulting in Serious Bodily Injury since June 27, 2023, including:

a. Conversations pertaining to the night of June 27, 2023, and time thereafter regarding the assault of AV1 and AV2.

b. Lists of customers and related identifying information.

c. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.

d. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information).

e. Any information recording Plazola's schedule or travel from June 27, 2023, to the present.

f. All bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet, including:

- a. Records of Internet Protocol addresses used.
 - b. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
 - c. Records of data storage accounts and use of data storage accounts.
4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Phone may require authorities to employ techniques, including imaging the Phone and computer-assisted scans and searches of the entire Phone that might expose many parts of the Phone to human inspection in order to determine whether it constitutes evidence as described by the warrant.
6. The initial examination of the Phone will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.
7. If, at the conclusion of the examination, law enforcement personnel determine

that particular files or file folders on the Phone or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Phone does not contain any data falling within the ambit of the warrant, the government will return the Phone to its owner within a reasonable period of time following the search and will seal any image of the Phone, absent further authorization from the Court.

9. If the Phone contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Phone as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phone and/or the data contained therein.

10. The government will retain a forensic image of the Phone for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.